World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Cyber-attacks and digital security: A review

Arati Sameer Nimgaonkar [1,*] and. Dr. Rajendra D. Kumbhar [2]

[1] *Research Scholar, Department of Computer Science, Tilak Maharashtra Vidyapeeth, Pune, India.*

[2] *Head, Department of Computer Science, KBPIMSR, Satara, India.*

World Journal of Advanced Engineering Technology and Sciences, 2023, 10(01), 103–107

Publication history: Received on 08 August 2023; revised on 17 September 2023; accepted on 20 September 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.10.1.0261

Abstract

In today's cyber world, information or data has the highest importance. So, it needs to be protected every time. The way we keep our valuable belongings in the locker on the same line data should be kept in the locker but at the same time it should be accessible whenever it is needed. But many a times, people who are part of this cyber world are not technical people. Information about users is being exchanged due to a growth in online communication utilizing various electronic devices including mobile phones, tablets, and other convenient forthcoming technologies. These links can make it simple to access the information of other users, which confirms the necessity of establishing trust and security in our everyday digital lives. Information security is the practice of using the proper procedural and technical controls to secure information and information systems, such as networks, data centers, and apps. This research study tries to give an overview of information security in terms of several methods for protecting data from threats and assaults.

Keywords: Information security; Network security measures; Cyber security; Confidentiality; Integrity; Availability, Non-repudiation; CIA; Attacks; Measures

1. Introduction

Our cyber space has changed and will continue to evolve as a result of system digitalization. They are essential to our security, wellbeing, and economic prosperity and have the potential to have a large positive impact on society. The Internet and computers are essential to many facets of our existence, such as communications, transportation, government, banking, healthcare, and education.

We will need a strong security system that includes safeguarding the data we depend on every day, whether at home, work, or school, to enjoy these benefits. The care and choices individuals make when they set up, manage, and utilise computers and the Internet are crucial to information security.

2. Information Security

We must be careful in protecting our systems and data against many assaults and risks brought on by the growing usage of the Internet, including scams, spoofing, sniffing, data theft, and other online vulnerabilities.

A typical computer connected to the Internet that lacks sufficient security measures can be hacked in a matter of seconds. Every day, thousands of malicious web sites are found. In data breaches, hundreds of millions of records were exposed. Attacks using zero-day vulnerabilities or SQL injection are two recent examples of new attack techniques. These are only a few instances of the dangers that emphasize the necessity of information security as a strategy.[2]

* Corresponding author: Arati Nimgaonkar

3. Digital security

"Problems cannot be solved with the same level of awareness that created them"- Albert Einstein i.e. the end users problems cannot be solved by more advanced technological solutions, but it has to be a combination of information technology and management skills used for it. More sophisticated technical solutions cannot be employed to tackle the problems of the end users; instead, management and information technology abilities must be combined. How do you ensure the security of transferred or stored data when we have to save our personal information on a computer or in datacenters? Cybersecurity is essential in this situation.[1]

Most individuals either keep their personal information on their own computer or on another person's. How are the systems on which the data lies (or is transported) and the data itself maintained secure?

They make the very incorrect assumption that anti-virus is equal to complete information or data security. They are unaware that there are several items on the market that can address risks. But it's astonishing what security improvements may be made almost for free by simply tightening up how we handle our computer systems.

The most frequently accepted definition of information security is a set of properties that must be maintained. Information security can be defined as the safeguarding of data for its confidentiality, integrity, and availability. Known colloquially as the CIA Triad of Security (BS7799/ISO17799, 1999). Information security influences how information is used. The CIA (Figure.-1) guides for the measurement of valuable information security. [4]

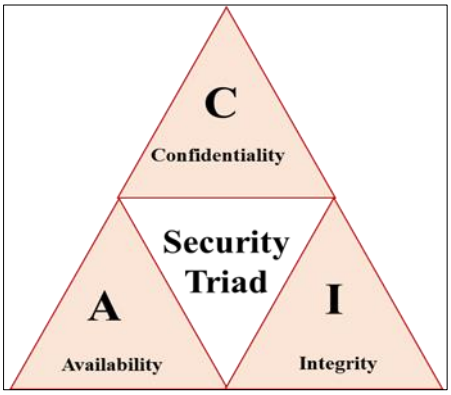

Figure 1 CIA Triangle

Confidentiality - The information should only be accessible to authorized users. In a nutshell, safeguarding sensitive information against unauthorized disclosure or understandable interception. only the intended recipient other than you can access that data.

Integrity - No one other than the authorized user should be able to make modifications to the information. In a nutshell, it ensures the accuracy and completeness of information and computer systems.

Availability - Authorised users should be able to access information when they require it. In a nutshell, ensuring that users have access to information and critical services when they need them.

One of the major drawbacks of CIA Triad is that it does not cover third-party activities like interception, repudiation, or misrepresentation. repudiation is the capacity of a third party to deny a prior interaction. Further, in 1998, The Parkerian Hexad is proposed by Donn B. Parker. Three additional elements are added to the CIA triad, Hence the name Perkerian Hexad. Figure-2 depicts the enhanced CIA Triad with newly added three more elements, Authenticity, Utility. And Possession.

Figure 2 Parkerian Hexad

In this new Parkerian Hexad [6] definitions of security are changed a little bit which states

- **Availability** - Usability of information for a definite purpose.
- **Utility** - Usefulness of information for a definite purpose.
- **Integrity** – The information's quality, readability, completeness, and wholeness remain unaltered from a previous condition.
- **Authenticity** - Validity, conformance, and genuineness of information.
- **Confidentiality** - Observation and knowledge disclosure are limited.
- **Possession** – The ownership, management, and capacity for use of information.

4. Common Security Threats / Attacks

With the development of more modern technology and increased Internet use, system users frequently lose crucial information, which results in attacks by unauthorized users. Attacks are attempts by unauthorized parties to gain access to or edit information, mislead the system so that they may commandeer an authorized session, or interfere with the service provided to authorized users. [5]

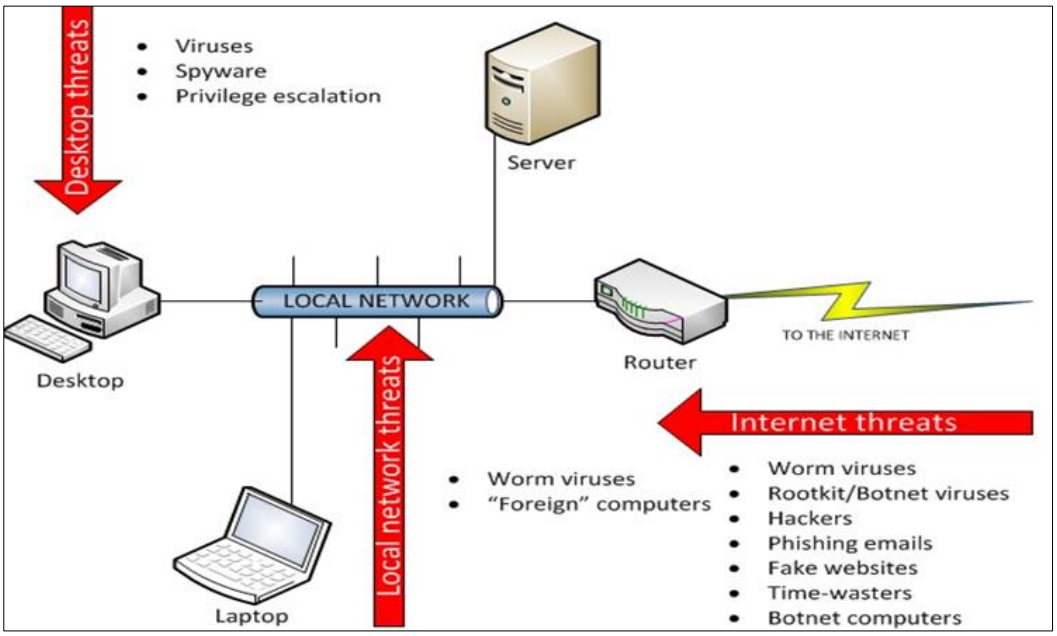

Figure 3 Threats and Attacks

Some generic threats are-

- Virus- A computer program created deliberately to damage a computer's data, applications, files, etc. It damages the computer and makes duplicates of itself.
- Eavesdropping- A computer, smartphone, or other connected device may steal information as it is being transferred over a network in an eavesdropping attack, often referred to as a sniffing or spying attack. Data that is being sent or received by the user can be accessed by the attack by taking advantage of unencrypted network traffic.
- Phishing: Through fraudulent email, phishers or invaders try to steal information. An attacker can pretend to be on any website in order to acquire login credentials or passwords.
- Insecure Wireless access point- Use of unknown broadband connections such as routers or any access point are also not safe to use, where user connects the wireless devices such as PDA's, mobiles and access the Internet.
- Spyware, Adware and Trojan- Spyware is regarded as a dangerous attack in which a hacker tracks a user's internet usage and installs a harmful program to collect personal data. Trojans and adware both function similarly. They obtain their information via free software obtained from the Internet, damaged CDs, and flashing advertisements. These programmes can be used by third parties to record the user's activities in detail, creating a profile without the user's knowledge.

5. Securing the Digital System

Specific precautions should be taken based on the kind of attack that will damage a system or the data inside it if it is attacked or at danger of being attacked. Basic techniques must be used to offer security or preventative measures for information. [3]

- Prevention: To prevent an attack on the information system or information itself, user should apply appropriate measures to it. The system should be prevented from or by the threats entering into it.
- Detection: The user of the information system should be sure about detecting a threat or kind of attack happened to the information. The designed system should be strong enough to detect it by generating any kind of notification or an alarm type to the user. In case of failure of prevention, user should get alerted as soon as possible.
- Reaction: Detecting the failure in the information system does not mean that system is secured if it does not have the ability to respond. Once the user detects a threat or attack happened to the information, system should have an effective counter measures to be taken on to it.

6. Preventive measures from attacks and threats:

- Regularly scan the system and keep updating the virus scanning tools/software.
- Avoid downloading contents from unsecure, unknown social engineering and networking sites
- Use of secure wireless networks
- Avoiding the pitfalls of online trading
- Reducing the Spam mail
- Use of preventive measures while using Digital Signature
- Using cautions while performing email attachments
- Use of SSL for end to end encryption
- Use of WPA (Wi-Fi Protected Access)
- Implement strict measures against unauthorized access
- Keep updating the software applications and patches
- Implementation of Firewall
- Web site certifications

7. Conclusion

The way Internet is more powerful and effective tool for communication, at the same time it is most vulnerable also. The security specification should include the security services that are needed and necessary for the users to access it.

The paper provides an insight to different security principles, attacks and he effective measures to be used against those attacks. Confidentiality, data integrity and availability are the important security framework that fulfills the user needs for secure system and in turn for a network as well.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare no conflict of interest.

References

[1] Peoples' role in Cyber Security , https://www.crucial.com.au/pdf/Peoples_Role_in_Cyber_Security.pdf

[2] Cyber Security is our shared responsibility http://cybersecurity.alabama.gov/Documents/security/WhyCyberSecurityisImportant.pdf

[3] Cyber Security it's just not about Technology https://assets.kpmg.com/content/dam/kpmg/pdf/2014/05/cyber-security-not-just-technology.pdf

[4] http://panmore.com/the-cia-triad-confidentiality-integrity-availability

[5] Classification of Network Attacks and Countermeasures of Different Attacks C. V. Anchugam and K. Thangadurai

[6] The Parkerian Hexad: The CIA Expanded, By Georgie Pender-Bey ,https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf